SEAN A. LINCOLN (State Bar No. 136387)
salincoln@orrick.com
I. NEEL CHATTERJEE (State Bar No. 173985)
nchatterjee@orrick.com
MONTE COOPER (State Bar No. 196746)
mcooper@orrick.com
THERESA A. SUTTON (State Bar No. 211857)
tsutton@orrick.com
YVONNE P. GREER (State Bar No. 214072)
ygreer@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400
Facsimile: 650-614-7401

Attorneys for Plaintiffs
THE FACEBOOK, INC. and MARK ZUCKERBERG

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

THE FACEBOOK, INC. and MARK ZUCKERBERG, Plaintiffs, v. CONNECTU, INC. (formerly known as CONNECTU, LLC), PACIFIC NORTHWEST SOFTWARE, INC., WINSTON WILLIAMS, WAYNE CHANG, and DAVID GUCWA, Defendants.	Case No. 5:07-CV-01389-RS **(CORRECTED) PLAINTIFFS' SECOND AMENDED COMPLAINT FOR VIOLATION OF CALIFORNIA PENAL CODE § 502(C); CALIFORNIA AND MASSACHUSETTS COMMON LAW MISAPPROPRIATION / UNFAIR COMPETITION; VIOLATION OF MASSACHUSETTS GENERAL LAW 93A; 18 U.S.C. § 1030; AND 15 U.S.C. §§ 7704 AND 7705**

Dockets.Justia.com

Plaintiffs Facebook, Inc. and Mark Zuckerberg hereby allege violations of California Penal Code section 502(c), the Computer Fraud and Abuse Act, the Federal Can-Spam Act of 2003, Massachusetts General Law 93A § 2, and Common Law Misappropriation / Unfair Competition under California and Massachusetts law, against Defendant ConnectU, Inc., Cameron Winklevoss, Tyler Winklevoss, Divya Narendra, Pacific Northwest Software, Inc., Winston Williams, Wayne Chang, David Gucwa, and Does 1-25 inclusive (collectively, the "Defendants"), as follows:

PARTIES, JURISDICTION, AND VENUE

1. Facebook, Inc. is a Delaware corporation with its principal place of business at 471 Emerson Street, Palo Alto, California. Facebook operates all of its servers in and/or from California and has done so since June 2004.

2. Mark Zuckerberg is an individual with a place of residence in the State of California.

3. On information and belief, Defendant ConnectU, Inc. (formerly known as ConnectU LLC) is incorporated in the State of Connecticut, with its principal place of business at 500 West Putnam Avenue, Greenwich, Connecticut. ConnectU was at all relevant times doing business in California. ConnectU is an interactive website that purports to provide certain website services to university students and alumni. ConnectU has specifically targeted California universities and students in its business activities. For example, ConnectU purports to have created "environments" for California universities, including but not limited to University of California, Berkeley. In addition, on information and belief, ConnectU sent commercial email to hundreds, if not thousands, of California residents. Its activities in California have been substantial and continuous.

4. Plaintiffs are informed and believe and thereupon allege that Defendant Cameron Winklevoss is a citizen of the State of Connecticut. Plaintiffs are informed and believe and thereupon allege that Defendant Mr. Winklevoss was a resident of the State of Massachusetts until at least June 2004. Mr. Winklevoss purports to be a founder of ConnectU. On information and belief, Mr. Winklevoss is and always has been an officer of ConnectU and held an equivalent

position with ConnectU's predecessor, ConnectU LLC. As described below, Mr. Winklevoss has, in his individual capacity, engaged in conduct designed to harm Plaintiffs, when he knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California.

5. Plaintiffs are informed and believe and thereupon allege that Defendant Tyler Winklevoss is a citizen of the State of Connecticut. Plaintiffs are informed and believe and thereupon allege that Mr. Winklevoss was a resident of the State of Massachusetts until at least June 2004. Mr. Winklevoss purports to be a founder of ConnectU. On information and belief, Mr. Winklevoss is and always has been an officer of ConnectU and held an equivalent position with ConnectU's predecessor, ConnectU LLC. As described below, Mr. Winklevoss has, in his individual capacity, engaged in conduct designed to harm Plaintiffs, when he knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California.

6. Plaintiffs are informed and believe and thereupon allege that Defendant Divya Narendra is currently a citizen of the State of Massachusetts. Plaintiffs are informed and believe and thereupon allege that Mr. Narendra was a citizen of New York until late 2006, and a resident of the State of Massachusetts from September 2000 through June 2004. Mr. Narendra purports to be a founder of ConnectU. On information and belief, Mr. Narendra is an officer of ConnectU and held an equivalent position with ConnectU's predecessor, ConnectU LLC. As described below, Mr. Narendra has, in his individual capacity, engaged in conduct designed to harm Plaintiffs, when he knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California. Mr. Narendra also personally hired at least one other person to assist in the conduct alleged herein.

7. Plaintiffs are informed and believe and thereupon allege that Defendant Pacific Northwest Software, Inc. ("PNS") is incorporated in the State of Washington, with its principal place of business at 2210 177th Place, NE Redmond, Washington. On information and belief, PNS has entered into contracts with California residents and has derived substantial revenue from California residents. For example, in 2005 PNS issued a press release in which it announced a web development deal with the Chula Vista Elementary School District (located in California),

pursuant to which PNS would develop internet "portals" for 50 sites (including 43 district schools) that would be available to the public. Plaintiffs are informed and believe and thereupon allege that ConnectU and/or its founders hired PNS to gain unauthorized access to Facebook's servers and website and to take, without permission, information found therein. Plaintiffs are informed and believe that PNS has entered into contracts in California, has clients in California, has received revenue from California residents, has solicited website users from California, has advertised in California, and has traveled to this state. As described below, PNS and its agents engaged in conduct designed to harm Plaintiffs, when they knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California.

8. Plaintiffs are informed and believe and thereupon allege that Defendant Winston Williams is a citizen of the State of Washington, and that he helped the Defendants develop a software application designed to hack into www.facebook.com and steal information. As described below, Mr. Williams has engaged in conduct designed to harm Plaintiffs, when he knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California. Mr. Williams has, at various times, been employed by ConnectU and PNS.

9. Plaintiffs are informed and believe and thereupon allege that Defendant Wayne Chang is a citizen of the State of Massachusetts, and that he was hired by ConnectU and/or its founders to gain unauthorized access to Plaintiffs' server and website and to misappropriate information found therein. As described below, Mr. Chang has engaged in conduct designed to harm Plaintiffs, when he knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California. Plaintiffs are informed and believe and thereupon allege that Defendant Chang is currently employed by Defendant PNS.

10. Plaintiffs are informed and believe and thereupon allege that Defendant David Gucwa is a citizen of the State of Massachusetts, and that he was hired by ConnectU and/or its founders and/or Defendant Chang to gain unauthorized access to Plaintiffs' server and website and to misappropriate information found therein. As described below, Mr. Gucwa has engaged in conduct designed to harm Plaintiffs, when he knew Plaintiffs were located in California and that the harmful effects would be felt by Plaintiffs in California.

11. Plaintiffs have not yet fully and independently identified the true names and capacities of the Defendants sued herein as Does 1-25, inclusive, and therefore sues those Defendants by such fictitious names. Plaintiffs reserve the right to amend this complaint to allege such Defendants' true names and capacities when they are ascertained. Plaintiffs are informed and believe and thereupon allege that each of the fictitiously designated Defendants has been acting as a partner, contractor, joint venturer, agent, or employee of one or more of the named Defendants and that each is jointly and severally responsible for the acts and omissions complained of herein.

12. Jurisdiction and venue are proper in this jurisdiction pursuant to Federal Rules of Civil Procedure Sections 1331, 1332, 1367, and 1391(b) and (c). The cause of action arose and the injuries described herein occurred primarily or wholly within the County of Santa Clara. The wrongful acts causing such injuries were initiated at various times from the States of Massachusetts, New York, and Connecticut and directed at persons and equipment in California.

GENERAL ALLEGATIONS

A. Mark Zuckerberg

13. Mark Zuckerberg is a former Harvard student who, in June 2004, took a leave of absence from school to come to California. He hoped to launch a successful business. He succeeded and decided to stay in California.

B. Facebook

14. Facebook is an interactive computer service that enables social networking amongst present and former university students. Plaintiffs have been operating the popular website, www.facebook.com,[1] from California since June 2004. During all relevant times herein, Plaintiffs are informed and believe that Defendants were aware that www.facebook.com operated from California.

15. Facebook is an industry leader in the business of social networking for college students. It currently has over 19 million registered users.

---

[1] The website was originally called www.thefacebook.com. To avoid confusion, Plaintiffs refer to the site by its current name.

16. In order to legally access user data and other specific information on Plaintiffs' website, one must register and thereby agree to Plaintiffs' Terms of Use ("Terms of Use") and its Privacy Policy ("Privacy Policy"). Plaintiffs have authorized access only to those individuals who agree to the Terms of Use. The use of any information on the Facebook website contrary to the Terms of Use is unauthorized. Enabling users of the Facebook website to control the level of privacy to their personal information is of utmost importance to Plaintiffs and the success of their business. Facebook users are expected to respect the privacy of other users and abide by the Privacy Policy and Terms of Use. During all relevant times herein, Defendants were aware of these policies.

17. The Terms of Use and the Privacy Policy have, at all times since the launch of Facebook's website, prohibited all commercial use and access to data and communications therein, except as explicitly authorized by Plaintiffs.

18. From at least February 2004, the Terms of Use provided as follows (aside, on information and belief, from non-substantive modifications):

> The Web site is for the personal use of individual Members only and may not be used in connection with any commercial endeavors. Organizations, companies, and/or businesses may not become Members and should not use the Service or the Web site for any purpose. Illegal and/or unauthorized uses of the Web site, including collecting email addresses or other contact information of members by electronic or other means for the purpose of sending unsolicited email and unauthorized framing of or linking to the Web site will be investigated, and appropriate legal action will be taken, including without limitation, civil, criminal, and injunctive redress."

(Emphasis added.) In addition, it provided that:

> You may not engage in advertising to, or solicitation of, other Members to buy or sell any products or services through the Service. You may not transmit any chain letters or junk email to other members. Although Thefacebook cannot monitor the conduct of its members off the Web site, it is also a violation of these rules to use any information obtained from the Service in order to harass, abuse, or harm another person, or in order to advertise to, solicit, or sell to any member without their prior consent.

Lastly, it affirmed:

> Thefacebook owns and retains all proprietary rights in the Web site and the Service. The Web site contains the copyrighted material, trademarks, and other proprietary information of Thefacebook, and its licensors. Except for that information which is in the public domain or for which you have been given written permission, you may not copy, modify, publish, transmit, distribute,

perform, display, or sell any such proprietary information.

19. By registering, and becoming a member, the user may have access to view the personal data of other users within his or her college (*i.e.*, other students and alumni), as well as to the personal data of friends at other schools who have explicitly granted such user access. Each user has the ability to add his or her own personal identifying information and determine who may view it. Such personal information may include his or her relationship status, birth date, phone numbers, email address, and home address. Each item of personal information is provided only by the user, and none of it is required in order to be a member of the website. At the relevant times, the default privacy setting on a user's account limited a user's access to a school network, but any user could have further limited access by selecting a more strict privacy setting such that only her confirmed friends could view her information. Even now, the default setting provides a limited view of a user's personal information, and the user has the option to make no information available publicly.

20. Plaintiffs also restrict access to and have always used their best efforts to keep their proprietary user and system information from unauthorized uses and parties.

21. Plaintiffs have generally expended substantial effort, money and time in developing the informational components of its website, as well as its aggregate user base. The data on the Plaintiffs' computers, computers systems, and computer networks is highly valuable.

22. At different times from the winter or spring of 2004 through at least 2005, Defendants Cameron and Tyler Winklevoss, Divya Narendra, Wayne Chang, Winston Williams, and David Gucwa knowingly circumvented the Terms of Use for the Facebook website by illicitly employing the user IDs and passwords of friends who were registered members of the Facebook website to mask Defendants' real identities. These defendants took these actions in order to gain access to the site and to steal information and data for commercial purposes, as well as to advertise to and solicit members of the Facebook website to join www.connectu.com. Both Defendants and the friends who provided Defendants with their user IDs and passwords did so cognizant that such use was intended to harm Plaintiffs. Defendants' actions were at all times intentionally aimed at, and the effects were felt by, Plaintiffs in California.

23. The users whose passwords Defendants (including, at least, Messrs. Winklevoss, Narendra, Chang, and Gucwa) used to knowingly and improperly access the Facebook website in California for commercial purposes and in violation of Plaintifffs' Terms of Use include, but were not limited to, user IDs and passwords associated with the email addresses carlsson@stanford.edu and stinab8@ucla.edu. The use of such user IDs and passwords for commercial purposes by Defendants in violation of Plaintiffs' Terms of Use harmed Plaintiffs in California. Defendants knew that such actions were improper, and that the harm would be uniquely felt by Plaintiffs in California.

B. Unauthorized Access, Misappropriation, and Commercial Use by Defendants

24. ConnectU offers an interactive computer service that purports to enable social networking amongst present and former university students.

25. ConnectU has attempted to aggressively compete with Facebook.

26. Beginning in 2004, and upon information and belief continuing through and including 2005, ConnectU and/or its founders hired PNS, Winston Williams, Wayne Chang, and David Gucwa to write software to gain access, without permission, to Plaintiffs' website and steal information, including email addresses and personal user information. ConnectU and/or its founders also requested that friends of the founders, such as Divya Narendra's friend Deva Mishra, attempt on behalf of ConnectU and the founders to violate Plaintiffs' Terms of Use and steal email addresses; personal user information such as birthdates, addresses, and phone numbers; course information; and other data from the Facebook website so that ConnectU could solicit Facebook users (including users of the Facebook website located in California) to join www.connectu.com. ConnectU, Messrs. Winklevoss and Narendra knew the harm from such activities would be felt by Plaintiffs in California. They directed their activities through third parties such as Deva Mishra knowing that the activities would result in the solicitation of California-based Facebook members to join the website www.connectu.com .

27. In the Spring 2004, Tyler and Cameron Winklevoss and Divya Narendra hired iMarc, a website developer, to help build the ConnectU website. On or around June 11, 2004, "the boyz from" ConnectU asked iMarc to

> write a little script that logs into www.thefacebook.com, loops through http: //www. thefacebook.com/profile.php?id=xxxxx replacing xxxxx with numbers to grab people's email addresses.

iMarc refused, because its employees believed that the request was unethical. Despite iMarc's caution against such activity, on July 22, 2004, "the boyz from" ConnectU "sent thousands of invite emails [over a 12 hour period]. Every single one was sent using a bogus 'From' address: … ."[2] For example, some of the "invite emails" purported to come from "god@harvard.edu." Many of these emails were sent to California college students via email addresses extracted from the Facebook website. The email addresses were obtained by ConnectU, Messrs. Winklevoss and Narendra through their illicit use of third party user accounts on the Facebook website. The "invite emails" did not indicate that they contained an advertisement for users to join a competing website, www.connectu.com. iMarc's relationship with ConnectU soured and ended shortly after this incident.

28. Messrs. Winklevoss engaged Wayne Chang, PNS and Winston Williams to develop a computer program designed to retrieve user account names, personal data (including email addresses and personal data of such user's "friends") from Facebook and its servers located in California. Mr. Chang hired David Gucwa, a computer programmer, to write the programs necessary to retrieve email accounts, course information and other data from the Facebook website and Plaintiffs' servers in California. Mr. Chang and Mr. Gucwa, with the knowledge and support of ConnectU, Cameron Winklevoss, Tyler Winklevoss, and Divya Narendra, collaborated with PNS and Mr. Williams to achieve the goal of writing programs to retrieve email account information, course information and other data from the Facebook website and its servers in California.

29. Mr. Chang, in aid of his "partners" Tyler Winklevoss, Cameron Winklevoss and Divya Narendra, provided Mr. Gucwa with fake and/or "borrowed" user accounts, including (but not limited to) stinab8@ucla.edu and carlsson@stanford.edu, and gave him specific instructions to play "cat and mouse" with Facebook. Mr. Chang noted that Facebook was "run by a techie," a

---

[2] All quotes in this complaint are taken directly from documents produced in response to discovery requests.

reference that upon information and belief was to California resident Mark Zuckerberg, so they should "be careful." Mr. Gucwa indeed wrote a "script" that worked in two steps: it retrieved the user ids and then the user profile information. It was a slow process, according to Mr. Gucwa, "because the program has to "descend" into each separate profile for each separate friend." Mr. Gucwa eventually "[w]rote a script that catches up to 10k [user i.d.s] at a time." Mr. Chang was pleased by this news because he wanted to "seed ConnectU as much as possible." The "good news," he said, "is that I'm sending thefacebook several thousand requests in a couple minutes and they haven't blocked my IP yet." Mr. Chang was concerned, of course, about setting off "huge" alarms at Facebook, and wondered how they could steal the information "faster." On January 27, 2005, Mr. Gucwa boasted that he had implemented the program he developed to collect 46,000 "ids" from the Facebook website.

30. The programs that Mr. Chang, Mr. Gucwa, Mr. Williams, and PNS developed in 2005 to misappropriate Facebook email account and other information so that ConnectU could spam Facebook users with invitations to join www.connectu.com were called variously "importer," "Facebook importer," "crawler," "grabFacebook.php," "grabFacebook2.php," and "Social Butterfly." Upon information and belief, ConnectU, Cameron Winklevoss, Tyler Winklevoss, and Divya Narendra knew about the actions of Mr. Chang, Mr. Gucwa. Mr. Williams, and PNS, were familiar with the importer, Facebook importer, crawler, grabFacebook.php, grabFacebook2.php, and Social Butterfly programs and their purposes, and were aware that the programs required access to Plaintiffs' servers in California in order for the programs to have their intended effects. Upon information and belief, the intended effects of these programs included, but were not limited to, crawling the Facebook website, illicitly importing without permission email addresses and personal user information into the www.connectu.com website, and soliciting via spam email with false and/or misleading header information Facebook users, including users located in California, to join the www.connectu.com website. Such misleading header information included false information suggesting that the invitation was not a commercial advertisement and that the spam request had originated as a result of the stated wishes of third parties. Instead, on information and belief, the commercial

advertisement emails were sent by Defendants.

31. Upon information and belief, among other methods Mr. Chang, Mr. Gucwa, Mr. Willams and PNS (with the support and knowledge of ConnectU, Cameron Winklevoss, Tyler Winklevss, and Divya Narenda) "spoofed" the Facebook website to gain access to email account and other information. Said "spoofing" was accomplished by using an email header or browser to make it appear as though the communication link originated from someone other than a source associated with Mr. Chang, Mr. Gucwa, Mr. Williams or PNS. Upon information and belief, Defendants "spoofed" the website to illicitly circumvent the Facebook website security measures designed to prevent parties such as Defendants from hacking into the Facebook website in order to steal data contained on the Facebook website and its California servers.

32. In February 2005, Mr. Chang was notified that his account had been suspended because the web service Defendants were using had received complaints from someone at Facebook that its California servers had been attacked through the web service. The web service indicated that it noticed a significant amount of activity and wondered what Defendants' interest in www.facebook.com was. In response, Mr. Chang notified defendants Cameron Winklevoss, PNS (through its CEO, John Taves), Mr. Williams, and Mr. Gucwa that Facebook learned of their activity. Mr. Chang described a method for working around the suspended account and asked Mr. Williams, Mr. Gucwa, PNS and others to provide thoughts on how best to work around Plaintiffs' website security mechanisms. Mr. Winklevoss then indicated to these other defendants that the "importer" script, designed to breach Facebook's security mechanisms in order to steal user data, was top priority for them.

33. In late 2004, Messrs. Winklevoss and Narendra hired defendants PNS and Williams to help develop the connectu.com website. PNS/Mr. Williams joined forces with Messrs. Chang and Gucwa to develop the "importer/crawler" program, as well as the Social Butterfly program. All Defendants knew the "importer/crawler" and Social Butterfly programs would be used to spam and solicit California-based and other users of the Facebook website to invite them to join the ConnectU website. On information and belief, all Defendants also knew that the "importer/crawler" and/or Social Butterfly programs employed misleading email header

information that failed to indicate the solicitation was a commercial advertisement and/or which failed to apprise the solicited Facebook account holder that the email had not actually been sent by the person from whom it appeared to be sent. In early 2005, Mr. Williams logged many hours developing the "importer" program and stealing millions of emails from www.facebook.com website, including emails of users located in California and known to Mr. Williams and the other Defendants to be associated with California schools. Much of his activity was targeted at California residents.

34. In 2004 and 2005, ConnectU, Messrs. Winklevoss, Narendra and Chang received multiple complaints related to the spamming of Facebook users. In March of 2005, ConnectU, Cameron Winklevoss, Tyler Winklevoss, and Divya Narendra were specifically informed by one or more of the other Defendants that "some person from thefacebook" identified how the "headers" used by ConnectU worked, and why the spamming of Facebook users (including those based in California) had generated complaints. Upon information and belief, the headers that Defendants were aware created these complaints were email headers originating from connectu.com, and were misleading because they did not identify the solicitations as commercial solicitations and did not accurately reflect that the email originated from the administrators of connectu.com rather than friends of the Facebook users who received the email.

35. Through its actions, ConnectU and the other Defendants gained unauthorized access to Plaintiffs' servers and network. They have stolen extensive amounts of proprietary and personal user data from Plaintiffs, including but not limited to user data such as email addresses and other personal identifying information collected in Plaintiffs' servers. The Defendants' actions, which included using other users' accounts and passwords (as well as fake accounts and passwords), violated Plaintiffs' Terms of Use and Privacy Policy. Defendants' actions affected thousands, if not millions, of individuals who had no direct contact or prior business relationship with ConnectU. Their actions had a direct effect on thousands of California residents, including (but not limited to) students at UCLA, the University of California at Berkeley and Stanford.

36. At the time of Defendants' unauthorized access, all users were required to register and abide by the website's Terms of Use and Privacy Policy. The Terms of Use in effect at the

time of Defendants' unauthorized access of the www.facebook.com prohibited use of the website for commercial endeavors. In addition, the Terms of Use prohibited the collection of email addresses or other contact information of Plaintiffs' members for the purpose of sending unsolicited e-mail, including unsolicited e-mail to California-based users of the Facebook website. Defendants' activity violated Plaintiffs' Terms of Use and Privacy Policy.

37. On information and belief, Defendants willfully and maliciously engaged in unauthorized access to, and unauthorized appropriation of, Plaintiffs' data, computers, computer systems, and computer networks, at least in part in the hope of gaining competitive advantage for ConnectU through such activities and to avoid the effort, time and money needed to develop such data, user lists, and other matter on its own. At the time of Defendants' unauthorized access via importer, Facebook importer, crawler, grabFacebook.php, grabFaceboo2.php, and the solicitation of Facebook users via Social Butterfly, Plaintiffs and/or their data, computers, computer systems and computer networks were principally located in California.

38. Defendants sought commercial gain and competitive advantage through their unauthorized access as explained, in May 2004, by Cameron Winklevoss to his father, when he described how he and his colleagues would steal course information and other data from www.facebook.com in order to launch connectu.com with as many or more schools than Facebook. Defendant Cameron Winklevoss explained to his father Howard Winklevoss, who encouraged him, that such theft would give them a competitive advantage over Plaintiffs without investing the time it took Plaintiffs to become successful.

39. As a result of these incidents of unauthorized access and unauthorized appropriations by Defendants, Plaintiffs were damaged, including being damaged in California.

40. As a result of their deliberate actions, Defendants improperly benefited from Plaintiffs' business efforts and established reputation, including its business efforts and established reputation in California, gaining substantial advantage from access and use of Plaintiffs' commercial and proprietary information.

41. At various times, Defendants distributed e-mails to members of www.facebook.com and otherwise sought to solicit Plaintiffs' members, including the solicitation

of California-based members and members with whom ConnectU had no prior or direct relationship, in an effort to lure them to www.connectu.com. ConnectU used the email addresses that had been gathered by and/or for ConnectU through Defendants' unauthorized access to and unauthorized appropriations from Plaintiffs' computers, computer systems, and computer networks to unjustly enrich ConnectU, and to spam and solicit Facebook users to join the website www.connectu.com.

42. In response to ConnectU's mass e-mailings and Defendants' other actions, Plaintiffs were forced to notify certain of its members of the apparent breach of their privacy by ConnectU, along with its agents and partners. Plaintiffs are informed and believe and thereupon allege that such notice damaged the trust their members placed in Plaintiffs and harmed Plaintiffs' business, including its business in California.

43. Plaintiffs are informed and believe and thereupon allege that each of the Defendants had knowledge of the wrongful acts described herein (including that such wrongful acts would harm Facebook in California), as well as their commercial purpose. Defendants carried out such wrongful acts willfully and maliciously.

44. Plaintiffs are informed and believe and thereupon allege that Defendants and/or those similarly situated may continue to engage in such unauthorized access and unauthorized appropriations in the future. In addition, Plaintiffs are informed and believe and thereupon allege that Defendants continue to exploit the misappropriated data for their own commercial benefit, to Plaintiffs' detriment. Plaintiffs do not have an adequate remedy at law.

45. Defendants were aware at all times from the summer of 2004 through the present that their actions would harm Plaintiffs in California. For instance, in January, 2006, Defendant Williams discussed with attorneys for ConnectU how many California student members of Facebook had been spammed by ConnectU through the combined use of the Facebook importer/crawler, grabFacebook.php/grabFacebook2.php, and Social Butterfly.

FIRST CAUSE OF ACTION
(Violation of California Penal Code § 502(c) – Against All Defendants)

46. Plaintiffs hereby reallege and incorporate by reference paragraphs 1 through 45,

inclusive, of this complaint as though fully set forth herein.

47. Defendants have knowingly and without permission accessed, caused to be accessed, and used Plaintiffs' computers, computer systems, computer networks, and data stored therein, in order to wrongfully obtain and control data, website components, and other information of monetary value.

48. Defendants have knowingly and without permission taken, copied, and made use of data from Plaintiffs' computers, computer systems, and computer networks, as well as taken and copied resident data.

49. Defendants have knowingly and without permission provided or assisted in providing a means of accessing Plaintiffs' computers, computer systems, and computer networks in violation of California Penal Code Section 502. Furthermore, Defendants have knowingly instructed others to access, use, and copy information from Plaintiffs' computers, computer systems, and computer networks, without permission.

50. Defendants' unauthorized access and use has damaged and caused loss to Plaintiffs.

51. Defendants' actions constitute violations of California Penal Code section 502(c).

SECOND CAUSE OF ACTION

(Common Law Misappropriation / Unfair Competition under Massachusetts and California Law– Against All Defendants)

52. Plaintiffs hereby reallege and incorporate by reference paragraphs 1 through 51, inclusive, of this complaint as though fully set forth herein.

53. Plaintiffs expended considerable time and money developing their commercially valuable user base (including account information), website components, network, and other information specified in this complaint ("Facebook's Information").

54. Defendants have taken such information and without authorization used, disclosed, and held out as their own Facebook's Information, without compensation to Facebook.

55. Defendants' unauthorized access, use and disclosure of Facebook's Information was the result of the deceptive and unfair actions described above.

56. As a consequence, Plaintiffs have been harmed. Plaintiffs are informed and

believe, and on that basis allege, that Defendants' acts and conduct constitute common law misappropriation / unfair competition and were carried out willfully, fraudulently, maliciously, and with the wanton disregard of Plaintiffs' rights, thereby entitling Plaintiffs to compensatory and punitive damages to be proven at trial.

THIRD CAUSE OF ACTION
(Violation of Massachusetts General Law 93A § 2 – Against All Defendants)

57. Plaintiffs hereby reallege and incorporate by reference paragraphs 1 through 56, inclusive, of this complaint as though fully set forth herein.

58. Defendants' actions in gaining unauthorized access to www.facebook.com, misappropriating data, and sending unsolicited emails are unlawful, unfair, and deceptive.

59. Plaintiffs have been harmed as a direct consequence of Defendants' unlawful actions.

60. Defendants' unlawful, unfair and deceptive actions are in violation of Massachusetts General Law 93A.

FOURTH CAUSE OF ACTION
(Violation of 15 U.S.C. §§ 7704(a)(1), (2), (3) and 7705 – Against All Defendants)

61. Plaintiffs hereby reallege and incorporate by reference paragraphs 1 through 60, inclusive, of this complaint as though fully set forth herein.

62. Defendants accessed Facebook's computer system without authorization and intentionally initiated the transmission of multiple commercial electronic mail messages through Plaintiffs' computer system. Said commercial electronic mail messages contained materially false and/or materially misleading header information. The header information was materially false and/or misleading because it included a technically accurate originating electronic mail address, domain name, and/or Internet Protocol address purporting to be from a particular Facebook user, but the access to the email address for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations.

63. Defendants initiated the transmission of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that the subject heading of their email solicitations to Facebook users would be likely to mislead a

recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message because the message did not indicate that Defendants sent the email, that the email was an advertisement to join www.connectu.com, or that the email was not initiated by the sender from whom it appeared to be initiated.

64. On information and belief, Defendants initiated commercial electronic mail messages that did not contain a functioning return electronic mail address (*e.g.*, god@harvard.edu, jstarr@georgetown.edu, jstarr@amherst.edu, and jstarr@dartmouth.edu) or other Internet-based mechanism, to provide the recipient to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from ConnectU, Messrs. Winklevoss and/or Narendra at the electronic mail address where the message was received.

65. ConnectU, Messrs. Winklevoss and Narendra promoted, or allowed the promotion of www.connectu.com in a commercial electronic mail message, the transmission of which is in violation of 15 U.S.C. § 7704 (a)(1) because they knew or should have known in the ordinary course of their business that www.connectu.com was being promoted in such a message; they received or expected to receive an economic benefit from such promotion; and they took no reasonable action to prevent the transmission.

66. Defendants knowingly and willfully collected electronic mail addresses and other information from www.facebook.com using automated means.

67. At the time of Defendants actions, Plaintiffs' website contained a notice that member electronic mail addresses were not to be given, sold, or otherwise transferred to any other party.

68. Defendants' actions constitute violations of the Federal Can-Spam Act of 2003, 15 U.S.C. § 7701 *et. seq*.

FIFTH CAUSE OF ACTION
(Violation of 18 U.S.C. § 1030 – Against All Defendants)

69. Plaintiffs hereby reallege and incorporate by reference paragraphs 1 through 68,

inclusive, of this complaint as though fully set forth herein.

70. Defendants knowingly and with intent to defraud accessed Plaintiffs' computers without authorization.

71. Defendants' conduct involved interstate communications.

72. Through their unauthorized access, Defendants obtained information of value from Plaintiffs' computers.

73. Defendants' actions were committed for the purpose of commercial advantage.

74. Defendants' actions damaged and caused loss to Plaintiffs.

75. Defendants' actions constitute violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

PRAYER FOR RELIEF

WHEREFORE, based upon the foregoing, Plaintiffs pray for the following relief:

1. An entry of judgment in favor of Plaintiffs and against all Defendants on all causes of action.

2. Compensatory, consequential, and incidental damages including, without limitation, compensatory damages reasonably incurred by Plaintiffs to verify that each incidence of Defendants' access did not alter, damage, or otherwise harm the integrity of Plaintiffs' computer systems, computer networks, computer programs, or the data stored thereon, pursuant to California Penal Code § 502(e)(1);

3. Exemplary and punitive damages in an amount to exceed $25,000, as provided by law, including exemplary damages under California Civil Code § 3426.3(c) and punitive damages under California Penal Code § 502(e)(4) (exemplary or punitive damages);

4. Economic damages under 18 U.S.C. § 1030 (a)(5)(B)(i);

5. Compensatory damages under 18 U.S.C. § 1030 (a)(4), including the cost of responding to Defendants' actions, conducting a damage assessment, and restoring the system to its condition prior to Defendants' actions, and revenue lost, cost incurred and other consequential damages incurred;

6. Statutory damages under 15 U.S.C. § 7701, *et seq.*;

7. Aggravated damages under 15 U.S.C. § 7701, in an amount not to exceed three times the amount of statutory damages available;

8. General damages in an amount to exceed $25,000;

9. An accounting to establish, and an order requiring disgorgement of, the sums by which Defendants have been unjustly enriched, at any time, including that resulting from Defendants' use of Facebook's Information;

10. Pre-judgment and post-judgment interest at the maximum rate allowed by law;

11. Injunctive relief which assures that any future misappropriation of Plaintiffs' commercial proprietary and other information be immediately stopped on the part of Defendants and other appropriate persons and/or entities, irrespective of whether any such Defendant, other person and/or entities is under the control of any (other) Defendant;

12. All injunctive relief allowed under California Penal Code § 502(c) *et seq*.

13. Further equitable relief in the most appropriate form that will have the effect of "undoing" any past and current misappropriations of Facebook's commercial proprietary and other information on the part of Defendants and other appropriate persons and/or entities, irrespective of whether under the control of any of Defendants;

14. Attorneys' fees and costs incurred by virtue of this action, if authorized by law – including attorneys' fees and costs authorized by California Penal Code § 502(e)(2); Civil Code § 1021.5; 15 U.S.C. § 7701 *et seq*., and

15. Such other relief, in law or equity, as the Court may deem just and appropriate in the circumstances.

JURY DEMAND

Plaintiffs hereby demand a trial by jury for all issues which may be tried by jury.

Dated: January 22, 2008

SEAN A. LINCOLN
I. NEEL CHATTERJEE
MONTE M. F. COOPER
THERESA A. SUTTON
YVONNE P. GREER
ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Theresa A. Sutton /s/

Theresa A. Sutton
Attorneys for Plaintiffs
FACEBOOK, INC. and MARK ZUCKERBERG